COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER

April 15, 2016

TO: Mitchell H. Katz, M.D., Director
Los Angeles County Health Agency

FROM: John Naimo
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW – HIGH DESERT REGIONAL HEALTH CENTER**

We have completed a review of the Department of Health Services (DHS) High Desert Regional Health Center's (HDRHC) compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.[1] On January 25, 2016, we provided your Department with our final draft report. HDRHC staff generally agreed with our findings and indicated that a formal exit conference was unnecessary.

Overall Summary

At the time of our review, HDRHC was substantially in compliance with each of the nine areas we assessed. We found no significant deficiencies in HDRHC's HIPAA and HITECH program, and accordingly have made no recommendations. A summary of our findings is attached.

Approach/Scope

Our approach and scope considered that HDRHC is the hub facility in the High Desert Health System, providing primary and specialty care services to residents of the Antelope Valley. HDRHC's current facility opened in June 2014.

We conducted a comprehensive on-site review to evaluate HDRHC's compliance with the HIPAA Privacy Rule and DHS' HIPAA policies and procedures that are pertinent to an outpatient facility. We met with DHS' Privacy Officer, as well as HDRHC's

[1] 45 Code of Federal Regulations (CFR) Parts 160 and 164

Administrator, Chief Information Officer (CIO), Medical Records Officer, and Personnel Officer. HDRHC's CIO is responsible for administering HDRHC's Privacy and Security Program, which includes HIPAA compliance.

Our review utilized the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Program Check List/Audit Tool* in evaluating HDRHC's compliance with the HIPAA Privacy Rule and DHS' HIPAA Privacy Rule policies and procedures. DHS management is responsible for establishing and maintaining effective internal compliance with the HIPAA regulations, and has oversight of the HIPAA program throughout their facilities, including HDRHC. We considered DHS' internal controls over their compliance program, DHS policies, and the HIPAA Privacy Rule requirements that could have a direct and material effect on HDRHC.

Our review covered the HIPAA Privacy Rule requirements for:

- Notice of privacy practices (NPP) for protected health information (PHI)
- Safeguards for PHI
- Training
- Complaint process
- Uses and disclosures requiring authorization
- Accounting for disclosures of PHI
- HITECH Act breach notification
- Appropriate access to electronic PHI (ePHI)
- Contingency plan

Our review also examined, on a limited basis, HDRHC's compliance with certain aspects of the Security Rule where there was cross-over with the HIPAA Privacy Rule. These included administrative, physical, and technical safeguards.

Results of Review

Notice of Privacy Practices for Protected Health Information

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the NPP. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the NPP in the facility in a clear and prominent location where individuals are likely to see it, as well as make the NPP available to those who ask for a copy.[2]

[2] 45 CFR § 164.520(c)

We observed that the current DHS NPP is posted and available in prominent locations near the various clinics' patient reception areas, which is where visitors of the facility are most likely to see it. In addition, the NPP is available on HDRHC's website. Our review of the website noted that it included a link to the NPP in both English and Spanish.

Currently, HDRHC maintains patient NPP acknowledgment forms in Quantim Clintegrity 360 (Quantim), an electronic file-tracking database. Hardcopy records have already been scanned and archived at an offsite location maintained by a non-County contractor. On November 1, 2015, HDRHC began maintaining an electronic copy of completed NPP acknowledgment of receipt forms in the Online Real-time Centralized Health Information Database (ORCHID), DHS' electronic medical record system.

We randomly selected and reviewed 20 patients' medical charts in Quantim to determine whether HDRHC obtained patients' NPP acknowledgments. We noted that three (15%) of the charts reviewed did not contain a signed NPP acknowledgment. HDRHC's Medical Records Officer indicated that the three patients for whom we could not find NPP acknowledgments are long-time patients whose forms may have been archived prior to HDRHC's recent efforts to convert all patient records into an electronic format. We determined that the files could not be retrieved from the offsite record storage contractor in a timely manner, and since more recent medical records all contained the required NPP acknowledgments, we did not request them. HDRHC should ensure that all future NPP acknowledgment forms are maintained in ORCHID.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI.[3] A covered entity must reasonably safeguard PHI and ePHI, and make reasonable efforts to prevent any intentional or unintentional use or disclosure that violates the HIPAA Privacy Rule.

During our review, we observed that employees must use a keycard to access restricted areas at HDRHC, and that keycards are built into HDRHC staff identification cards. HDRHC's keycard system records the identity of each person who scans their card for access, as well as the date and time of access.

HDRHC primarily uses electronic medical records, and only two clinics still use paper charts. One of these clinics has its own medical records room. HDRHC also has a second medical records room for all other physical records. Both medical records rooms are located in restricted areas. According to HDRHC management, medical records rooms are accessible only by assigned staff, and access is restricted to those with a keycard.

[3] 45 CFR § 164.530(c)

Patients requesting records are directed to a window near the primary medical records room, and are given pagers to alert them when their records are ready for pick-up. This allows patients to wait in public waiting areas away from the medical records room.

We observed that computer monitors near public areas are equipped with privacy screens and are positioned away from public view so that the information is not readable. Fax machines, printers, and copiers are kept in secure areas and away from visitors. It appears that the workstations are compliant with the HIPAA standards.

HDRHC does not utilize patient sign-in sheets. Patients check-in with staff at various registration windows before they are directed to designated waiting areas for their appointments. Patients are escorted by staff through restricted areas to examination rooms.

HDRHC's CIO stated that the facility's computers are password protected and will automatically log out users after 15 minutes of inactivity. HDRHC's CIO further stated that passwords are changed every 90 days, in accordance with DHS policy. Employees are notified and periodically reminded to not store ePHI on hard drives. Staff are granted access to ePHI by management based on each employee's job function. ORCHID has the ability to limit access to certain fields containing ePHI based on the staff's business need and role. Thus, it appears that HDRHC is compliant with the security standards for password protections.

HDRHC has an on-site pharmacy. Per California Business and Professions Code §4116, no person other than a pharmacist, intern pharmacist, authorized officer of the law, or person authorized to prescribe shall be permitted into the area where controlled substances or dangerous drugs are stored, prepared, dispensed, etc. According to HDRHC management, HDRHC's pharmacy is secured with an alarm system which only pharmacists have the access code to disarm. Thus, it appears that the pharmacy maintains physical security that is compliant with both federal and State regulations.

It appears that HDRHC has implemented appropriate safeguards for PHI.

Training

A covered entity must train all members of its workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules to the extent necessary and appropriate for the members of its workforce to carry out their functions. Members of the workforce include employees, volunteers, and trainees.[4]

Prior to our review, we were informed that all HDRHC workforce members have received training on the HIPAA Privacy and Security Rules, HITECH Act's Breach

[4] 45 CFR § 164.530(b)

Notification Rule, and DHS' HIPAA policies and procedures through DHS' web-based training. Initial HIPAA training is also provided by DHS' Human Resources Division during new employee orientation via a handbook format. Refresher training is provided on an as-needed basis, and during re-orientation training and employee evaluations.

We obtained a HIPAA training status report as of October 8, 2015, from DHS' Privacy Officer, and noted that 441 of the 444 current HDRHC employees have completed DHS' HIPAA training. At the time of our review, one employee had been on long-term leave since June 2013 and one employee was a recent hire and did not have access to the online training modules. According to DHS' Privacy Officer, the third employee received copies of DHS' HIPAA policies during her orientation with DHS prior to her actual start date in May 2015, satisfying the requirement for HIPAA training, but did not complete her formal HIPAA training until October 8, 2015, which was not in time to be reflected in the status report. It appears that HDRHC is compliant with the HIPAA training standards.

Complaint Process

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.[5]

All HDRHC staff have access to DHS' complaint form via the DHS Intranet site, and can print a copy upon request. According to DHS Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI),* complaints are forwarded to HDRHC's CIO.

We reviewed HDRHC's HIPAA privacy investigation process and complaint investigation log. Between October 2014 and October 2015, HDRHC received one HIPAA complaint that was resolved within 60 days. It appears that HDRHC has an appropriate complaint process and they are documenting and maintaining a log of all complaints received, which include issues pertaining to patients' rights. HDRHC's complaint process and methods appear to comply with the HIPAA regulations.

Uses and Disclosures Requiring Authorization[6]

The U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) guidance defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or healthcare operations, or to disclose PHI information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the PHI to be used and disclosed, the person authorized to

[5] 45 CFR § 164.530(d)
[6] 45 CFR § 164.508(a)

make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

HDRHC management reported that they follow DHS Policy 361.3, *Use and Disclosure of Protected Health Information (PHI) Without Authorization,* which addresses uses and disclosures requiring an authorization from patients or their legal representatives and adhere to the policies. Our review of the policy and authorization form noted that they meet the uses and disclosures requiring authorization standard.

During our on-site review, we noted that three medical charts, which came from the above-mentioned 20 medical charts, contained signed authorization forms, which were completed according to HIPAA standards. Only medical charts that were subject to a disclosure requiring authorization will contain an authorization form.

Accounting for Disclosures of Protected Health Information

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity. Covered entities are required to account to individuals for certain non-routine disclosures of PHI. The HIPAA Privacy Rule gives individuals the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure.[7] The types of disclosures that are not required to be reported are disclosures:

- to the individual
- for treatment, payment, and healthcare operations
- for facility directories
- pursuant to authorization
- pursuant to a limited data set agreement
- to persons involved in the individual's care
- for correctional institutions
- for certain law enforcement purposes

As of November 1, 2015, all disclosures of PHI are tracked electronically through ORCHID. HDRHC management is aware that tracking for all disclosures must be maintained, with the exceptions described above, for a minimum of six years. HDRHC management stated that they have not received a request for an accounting of disclosures, which is common throughout the healthcare industry.

[7] 45 CFR § 164.528(a)

HITECH Act Breach Notification

HHS issued regulations requiring healthcare providers, health plans, and other entities covered by HIPAA to notify individuals when their health information is breached.[8] These "breach notification" regulations implement provisions of the HITECH Act, passed as part of the American Recovery and Reinvestment Act of 2009. The regulations developed by OCR require healthcare providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

All DHS Workforce members are required to follow DHS Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI),* which provides procedures for workforce members to follow when they encounter a potential privacy and/or security breach.

The HIPAA Compliance Unit worked with HDRHC's CIO to manage a prior data breach, and HDRHC responded professionally and competently to the incident.

Appropriate Access to ePHI

The Security Rule requires covered entities to have policies and procedures to ensure that workforce members have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI.[9]

DHS Policy 935.15, *System Audit Controls*, addresses controls to record and examine system activity for all electronic information systems. As of November 1, 2015, HDRHC began using ORCHID to access ePHI. DHS' Privacy Officer stated that in order to access ORCHID, users are required to authenticate to the system, and that the system maintains session logs, rights, and other tools to ensure appropriate access to DHS' data. DHS' Privacy Officer stated that access is determined by the user's role and assignment. We reviewed DHS' policy, which adequately addresses workforce access to ePHI.

Contingency Plan

The Security Rule includes requirements for covered entities to ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit. The Security Rule further requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

[8] 45 CFR §§ 164.400-414
[9] 45 CFR § 164.308(a)(3)(i)

Other provisions require policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. Contingency plans must be implemented and tested.[10]

DHS Policy 935.07, *Facility IT Contingency Plan*, details the requirements that HDRHC must follow to be compliant with HIPAA regulations. In addition, HDRHC's CIO stated that HDRHC possesses its own power generators, which can be started in approximately eight seconds in the event of a power failure.

ORCHID data is encrypted and replicated between two data centers located remotely and maintained by Cerner, a non-County contractor. It appears that HDRHC is compliant with the HIPAA standards for contingency planning.

Conclusion

Overall, we found that HDRHC appears to be compliant with the regulations we reviewed. We shared our findings with DHS and HDRHC management on January 25, 2016. We thank DHS' Privacy Officer, HDRHC's Administrator, CIO, Medical Records Officer, Personnel Officer, and staff for their cooperation and assistance with this review.

If you have any questions, please call me, or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166.

JN:AB:PH:RGC:LTM:TW

Attachment

c: Sachi A. Hamai, Chief Executive Officer
Mary C. Wickham, County Counsel
Audit Committee
Health Deputies

[10] 45 CFR § 164.308(a)

HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW
HIGH DESERT REGIONAL HEALTH CENTER
SUMMARY OF FINDINGS

The following table summarizes High Desert Regional Health Center's compliance in each of the nine areas we assessed during our review:

Regulations	Results
Notice of Privacy Practices (NPP) for Protected Health Information (PHI) – 45 CFR § 164.520(c)	Compliant
Safeguards for PHI – 45 CFR § 164.530(c)	Compliant
Training – 45 CFR § 164.530(b)	Compliant
Complaint Process – 45 CFR § 164.530(d)	Compliant
Uses and Disclosures Requiring Authorization – 45 CFR § 164.508(a)	Compliant
Accounting for Disclosures of PHI – 45 CFR § 164.528(a)	Compliant
HITECH Act Breach Notification – 45 CFR § 164.400-414	Compliant
Appropriate Access to Electronic PHI – 45 CFR § 164.308(a)(3)(i)	Compliant
Contingency Plan – 45 CFR § 164.308(a)	Compliant